R E P U B L I Q U E F R A N Ç A I S

Rec'd PCT/PTO 04 APR 2005 PCT/FR03/02854

10/530203

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REC'D 05 DEC 2003
WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 01 OCT. 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA RÈGLE 17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

bis, rue de Saint Pétersbourg
800 Paris Cedex 08
éphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle – Livre VI

N° 11354*02

REQUÊTE EN DÉLIVRANCE
page 1/2

Cet imprimé est à remplir lisiblement à l'encre noire — DB 540 W / 010802

Réservé à l'INPI

EMISE DES PIÈCES
ATE
IEU 4 OCT 2002
75 INPI PARIS
° D'ENREGISTREMENT
ATIONAL ATTRIBUÉ PAR L'INPI 0212340
ATE DE DÉPÔT ATTRIBUÉE
AR L'INPI – 4 OCT. 2002

Vos références pour ce dossier *(facultatif)*
BIF114642/FR

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BONNET-THIRION
12, avenue de la Grande Armée
75017 PARIS

2 NATURE DE LA DEMANDE — Cochez l'une des 4 cases suivantes

Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date
ou demande de certificat d'utilité initiale	N°	Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Carte à microcircuit dont les performances peuvent être modifiées après personnalisation.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☐ **Personne morale** ☐ **Personne physique**

Nom ou dénomination sociale		OBERTHUR CARD SYSTEMS SA
Prénoms		
Forme juridique		Société anonyme
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	102, Boulevard Malesherbes,
	Code postal et ville	7 5 0 1 7 PARIS
	Pays	FRANCE
Nationalité		FRANCAISE
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

R2

Réservé à l'INPI	
REMISE DES PIÈCES DATE	
LIEU	4 OCT 2002 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI	0212340

DB 540 W /300301

Vos références pour ce dossier : *(facultatif)*	BIF114642/FR
6 MANDATAIRE	
Nom	
Prénom	
Cabinet ou Société	CABINET BONNET-THIRION
N °de pouvoir permanent et/ou de lien contractuel	
Adresse — Rue	12 AVENUE DE LA GRANDE ARMEE
Adresse — Code postal et ville	7 5 0 1 7 PARIS
N° de téléphone *(facultatif)*	01 53 81 17 00
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	
7 INVENTEUR (S)	
Les inventeurs sont les demandeurs	☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE	**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé	☒ ☐
Paiement échelonné de la redevance	**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES	**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes	

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)	**VISA DE LA PRÉFECTURE OU DE L'INPI**
Bruno QUANTIN N°92-1206 CABINET BONNET-THIRION	M. ROCHET

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

La présente invention concerne une carte à microcircuit dont les performances peuvent être modifiées après une étape de personnalisation de la carte, et un procédé de configuration d'une telle carte.

Dans la suite de ce document, le terme *"personnalisation"* (ou individualisation) sera compris comme étant celui utilisé couramment par l'homme du métier dans l'industrie des cartes à microcircuit, ou tel que défini par W.Rankl et W.Effing dans le document *"Smart Card Handbook, Second Edition, Ed. John Wiley & Sons, Ltd"* de la façon suivante :

"Le terme personnalisation, dans son sens le plus large, signifie que les données spécifiques à une carte ou à une personne sont entrées dans la carte. Ces données peuvent par exemple être un nom, une adresse, mais aussi des clefs associées à la carte. La seule chose qui importe est que ces données soient spécifiques à cette carte."

L'invention trouve une application privilégiée, mais non limitative, dans le domaine des cartes à microcircuit de télécommunication mobile telles que les cartes SIM conformes à la norme GSM ou des cartes conformes à des normes similaires telles que les normes CDMA, TDMA ou UMTS. Dans ce contexte, l'invention permet la modification des performances d'une carte de télécommunication mobile personnalisée et déjà attribuée à un utilisateur abonné à un service de téléphonie mobile.

La modification de la fréquence d'horloge d'une carte à microcircuit est déjà connue de l'homme du métier lorsqu'elle s'effectue avant l'étape de personnalisation de la carte.

Un tel procédé est en particulier utilisé pendant les phases de développement d'une carte à microcircuit, phases au cours desquelles les cartes sont testées avec différentes fréquences d'horloge, la fréquence d'horloge de la carte étant ensuite figée avant la fin de la personnalisation.

Néanmoins, selon l'art antérieur, la modification des performances de la carte ne peut se faire après la personnalisation de la carte.

Il serait pourtant souhaitable de pouvoir modifier les performances d'une carte à microcircuit après personnalisation, notamment après sa commercialisation, ou plus généralement après qu'elle a été attribuée à un utilisateur.

A cet effet, l'invention concerne une carte à microcircuit comportant des moyens de réception d'une commande et des moyens de modification d'au moins une performance de la carte sur réception de la commande, les moyens de modification pouvant être mis en œuvre après une étape de personnalisation de la carte.

Corrélativement, l'invention vise, selon un deuxième aspect, un procédé de configuration d'une carte à microcircuit comportant les étapes successives suivantes :

- personnalisation de la carte ;
- réception d'une commande ; et
- modification d'au moins une performance de la carte sur réception de la commande.

Dans le contexte de la présente invention, une performance d'une carte à microcircuit pouvant être modifiée par un procédé de configuration conformément à la présente invention doit être comprise comme étant toute caractéristique matérielle ou logicielle préexistant dans la carte et non accessible après personnalisation.

L'invention permet ainsi d'améliorer ou de dégrader une performance d'une carte à microcircuit par l'envoi de la commande précitée après personnalisation, la carte étant déjà attribuée à un utilisateur. Sans la présente invention en revanche, un utilisateur souhaitant utiliser une carte avec des performances nouvelles doit nécessairement changer de carte à microcircuit.

Ainsi, l'utilisateur d'une carte à microcircuit comportant une mémoire physique EEPROM de 64 kilo-octets mais dont la taille de la zone utilisable a été limitée à 32 kilo-octets avant personnalisation, peut, sur

réception de la commande, bénéficier de la totalité des 64 kilo-octets de la mémoire physique sans avoir à changer de carte.

Selon une caractéristique avantageuse, la carte à microcircuit comporte en outre des moyens d'authentification d'un émetteur de la commande.

Dans un mode préféré de réalisation, ces moyens d'authentification comportent des moyens cryptographiques permettant de vérifier si la commande a été cryptée avec une clef d'authentification prédéterminée.

Ces moyens de vérification peuvent utiliser une fonction de hachage selon un algorithme du type MD4, MD5 ou SHA-1.

Ainsi, selon cette caractéristique avantageuse, les modifications de performance de la carte nécessitent la connaissance de la clef d'authentification, cette clef pouvant être gardée secrète par un opérateur, le fabricant de la carte ou tout tiers qui se réserve ainsi la possibilité de modifier les performances de la carte.

Dans une variante de réalisation, la clef d'authentification précitée est associée à la modification d'une performance prédéterminée d'une carte prédéterminée.

Selon une autre caractéristique, les moyens de modification sont adaptés à déterminer quelle performance de la carte doit être modifiée en fonction d'un ordre prédéterminé reçu dans la commande.

Cette caractéristique permet, selon l'ordre prédéterminé reçu dans la commande, de modifier une ou plusieurs caractéristiques de la carte.

Selon un mode de réalisation particulièrement avantageux, les moyens de réception sont adaptés à recevoir la commande selon le protocole SMS ou similaire tel que le protocole MMS (multimedia service).

Ce mode de réalisation permet ainsi la modification d'au moins une performance de la carte à travers un réseau de télécommunication mobile.

Bien entendu, dans d'autres modes de réalisation, la commande peut être reçue par les moyens de réception à travers un réseau filaire ou localement.

Selon un mode de réalisation préféré de la carte selon l'invention, les moyens de modification sont adaptés à modifier la taille d'une zone utilisable d'une mémoire physique de la carte.

Cette caractéristique permet ainsi d'augmenter les capacités de mémorisation de la carte, par exemple pour permettre le téléchargement de nouvelles applications dans la carte.

Dans une variante préférée de ce mode de réalisation, la modification de la taille de la zone utilisable de la mémoire physique est effectuée en créant ou en détruisant au moins un fichier spécifique compris dans la mémoire physique, ou en modifiant la taille d'au moins un fichier spécifique compris dans la mémoire physique.

Ce fichier peut être un fichier spécifiquement créé pour occuper un espace de la mémoire physique ou un fichier de données utilisé par une application de la carte à microcircuit.

Dans un autre mode de réalisation préféré, les moyens de modification d'au moins une performance sont adaptés à modifier, de façon réversible ou non une fréquence d'horloge de la carte.

Selon cette caractéristique particulière, on peut accélérer la vitesse de calcul d'un processeur ou d'un composant cryptographique de la carte, ce qui permet de réaliser des traitements plus complexes sur des données numériques reçues par la carte à microcircuit.

Dans un autre mode de réalisation, les moyens de modification d'au moins une performance sont adaptés à permettre ou empêcher, de façon réversible ou non, l'utilisation d'au moins une fonction logicielle de la carte.

Cette caractéristique particulière permet ainsi de valider des applications logicielles prévues initialement sur la carte mais invalidées avant la fin de sa personnalisation.

Une telle fonction logicielle peut par exemple être une fonction cryptographique telle qu'une fonction de contrôle d'une signature de données numériques.

De la même façon, dans un autre mode de réalisation, les moyens de modification de performance de la carte sont adaptés à permettre ou

empêcher, de façon réversible ou non, l'utilisation de tout ou partie d'un circuit électronique de la carte, ce circuit électronique pouvant par exemple être une unité cryptographique.

Les traitements cryptographiques qui étaient réalisés par logiciel peuvent ainsi avantageusement être accélérés par l'utilisation de cette unité cryptographique.

Dans un mode préféré de réalisation, la carte à microcircuit selon l'invention comporte en outre des moyens de synchronisation adaptés à vérifier l'unicité de la commande.

Cette caractéristique particulière permet avantageusement d'éviter une utilisation malhonnête de la carte à microcircuit en empêchant qu'une commande déjà reçue et copiée frauduleusement ne soit prise en compte une deuxième fois.

Les avantages et caractéristiques particulières propres au procédé de configuration selon l'invention étant similaires à ceux exposés ci-dessus concernant la carte à microcircuit conforme à l'invention, ils ne seront pas rappelés ici.

D'autres aspects et avantages de la présente invention apparaîtront plus clairement à la lecture des descriptions d'un mode particulier de réalisation qui va suivre cette description étant donnée à titre d'exemple non limitatif est faite en référence aux dessins annexés sur lesquels :

- la figure 1 représente de façon schématique l'architecture d'une carte à microcircuit conforme à l'invention ;
- la figure 2 représente une commande conforme à la présente invention, dans un mode préféré de réalisation ; et
- la figure 3 représente, sous forme d'organigramme, les principales étapes d'un procédé de configuration conforme à l'invention, dans un mode préféré de réalisation.

La **figure** 1 représente de façon schématique l'architecture d'une carte à microcircuit 100 conforme à l'invention.

La carte à microcircuit 100 comporte principalement un processeur CPU associé de façon classique à un certain nombre de mémoires de type RAM, ROM et EEPROM.

La mémoire ROM comporte en particulier les instructions d'un programme informatique adapté à mettre en œuvre un procédé de configuration conforme à la présente invention et dont les principales étapes seront décrites ultérieurement en référence à la figure 3.

De même, la mémoire vive RAM comporte des registres nécessaires à l'exécution de ce programme.

La carte à microcircuit 100 comporte également une mémoire physique, par exemple une mémoire de type EEPROM, dont la taille d'une zone utilisable 110 peut être modifiée après personnalisation.

La carte à microcircuit 100 comporte également un circuit électronique 120, constitué dans le mode de réalisation décrit ici par une unité cryptographique.

De façon connue, la carte à microcircuit 100 reçoit également un signal d'une horloge CLOCK externe à la carte, ce signal d'horloge étant fourni aux différents composants de la carte.

Dans le mode de réalisation particulier décrit ici, la carte à microcircuit 100 comporte un composant de type PLL (Phase Lock Looping en anglais) connu de l'homme du métier et permettant de dériver des signaux à différentes fréquences d'horloge, à partir du signal de l'horloge externe CLOCK.

Plus précisément, dans le mode de réalisation décrit ici, la zone utilisable 110 de la mémoire EEPROM comporte un registre mult_horl pour mémoriser un facteur multiplicateur appliqué à la fréquence du signal de l'horloge externe CLOCK.

A la mise sous tension de la carte à microcircuit, le processeur CPU lit ce registre mult_horl et programme le composant PLL avec la valeur contenue dans ce registre, le signal d'horloge en sortie du composant PLL étant ensuite appliqué à certains composants de la carte.

Dans le mode de réalisation décrit ici, le composant PLL permet ainsi de modifier la vitesse de calcul du processeur CPU et de l'unité cryptographique 120.

La carte à microcircuit 100 selon l'invention comporte des moyens de réception RX d'une commande 200 qui va maintenant être décrite, dans un mode préféré de réalisation, en référence à la **figure 2**.

La commande 200 comporte un champ 210 comportant un ordre prédéterminé dont l'analyse permet de déterminer quelles sont les performances de la carte 100 qui doivent être modifiées.

Dans l'exemple de réalisation décrit ici, les performances de la carte à microcircuit 100 pouvant être modifiées après personnalisation sont, la taille de la zone utilisable 110 de la mémoire physique EEPROM, la fréquence du signal d'horloge, une fonction logicielle f mise en œuvre par le processeur CPU et le circuit électronique 120.

Dans le mode de réalisation préféré décrit ici, l'ordre 210 est constitué par un octet dont :

- le premier bit (bit1) et le deuxième bit (bit2) sont représentatifs d'un ordre de création ou de destruction d'une zone utilisable 110, ou d'un ordre de modification de la taille de la zone utilisable 110 de la mémoire physique EEPROM de la carte à microcircuit 100 ;
- le troisième (bit3) et le quatrième bit (bit4) constituent un facteur multiplicateur de la fréquence du signal d'horloge fourni par l'horloge externe CLOCK ;
- le cinquième bit (bit5) est représentatif d'un ordre d'utilisation ou de non utilisation d'une fonction logicielle f de la carte ;
- le sixième bit (bit6) est représentatif d'un ordre d'utilisation ou de non utilisation du circuit électronique 120 ; et
- les septième et huitième bits sont non utilisés.

Dans le mode préféré de réalisation décrit ici, les moyens de réception RX sont adaptés à recevoir la commande 200 selon le protocole SMS, par exemple au moyen de la commande ENVELOPE de ce protocole, et à mémoriser cette commande 200 dans une zone de la mémoire vive RAM.

La carte à microcircuit 100 comporte également des moyens d'authentification d'un émetteur de la commande 200.

Dans un mode préféré de réalisation, les moyens d'authentification comportent des moyens cryptographiques permettant de vérifier si la commande 200 a été cryptée avec une clef d'authentification AUTH prédéterminée, la clef d'authentification AUTH étant mémorisée dans une partie AUTH de la zone utilisable 110 de la mémoire EEPROM au moment de la personnalisation de la carte.

Ces moyens cryptographiques peuvent être constitués par un programme informatique exécuté par le processeur CPU, ce programme informatique comportant des instructions de mise en œuvre d'un algorithme de décryptage à clef publique tel que l'algorithme RSA connu de l'homme du métier.

Dans le mode préféré de réalisation décrit ici, la carte à microcircuit 100 comporte en outre des moyens de synchronisation 130 adaptés à vérifier l'unicité de la commande 200, de façon à éviter qu'une commande 200 déjà reçue et copiée frauduleusement ne soit prise en compte une deuxième fois de façon non autorisée.

Les moyens de synchronisation 130 peuvent en particulier être constitués par un circuit électronique mettant en œuvre le test E35 de vérification décrit ultérieurement en référence à la figure 3.

Selon un mode préféré de réalisation, le processeur CPU détermine, à partir de la commande 200, la ou les performances de la carte à microcircuit 100 qui doivent être modifiées.

En particulier, si le couplet (bit1, bit2) constitué par le premier bit bit1 et le deuxième bit bit2 de l'ordre 210 est égal à (1,1), cela signifie que la taille de la zone utilisable 110 de la mémoire physique EEPROM doit, si possible être augmentée.

En pratique, et dans le mode de réalisation préféré décrit ici, la carte à microcircuit 100 comporte, avant personnalisation, un fichier informatique FICHIER_VOID dans la mémoire physique EEPROM de telle sorte que lorsque le couplet (bit1, bit2) est égal à (1, 1), le processeur CPU détruit ce

fichier FICHIER_VOID libérant ainsi une partie de la mémoire physique EEPROM.

En variante, lorsque le couplet (bit1, bit2) est égal à (1,1), la taille de la zone utilisable de la mémoire physique EEPROM est (si possible) augmentée en diminuant la taille du fichier FICHIER_VOID de façon prédéterminée, par exemple de 16 kilo-octets.

De même, dans le mode préféré de réalisation décrit ici, lorsque le couplet (bit1, bit2) est égal à (0,0), cela signifie que la taille de la zone utilisable 110 de la mémoire physique EEPROM doit si possible être diminuée, cette opération étant réalisée en augmentant (si possible) la taille du fichier FICHIER_VOID de façon prédéterminée, par exemple de 16 kilo-octets.

En variante, lorsque le couplet (bit1, bit2) est égal à (0,0), cela signifie qu'un fichier FICHIER_VOID doit être créé, si possible, à une adresse et avec une taille prédéterminées dans la mémoire physique EEPROM.

Dans le mode de réalisation décrit ici, la réception d'une commande 200 dont le couplet (bit1, bit2) est égal à (1,0) ou (0,1) est sans effet.

Conformément à la norme ISO7816, la modification des caractéristiques (création, destruction, changement de taille) du fichier FICHIER_VOID peut nécessiter une clef CLEF spécifique 220 reçue dans la commande 200, tel que représenté à la figure 2.

Dans un autre mode préféré de réalisation, plusieurs fichiers du même type peuvent être prévus avant personnalisation de la carte, ce qui permet d'augmenter, progressivement, par destruction de ces fichiers la taille de la zone utilisable de la mémoire physique EEPROM.

D'autre part, lorsque la carte à microcircuit 100 reçoit l'ordre 210, le processeur CPU obtient, par lecture du troisième bit3 et quatrième bit4 bits de cet ordre 210, un facteur multiplicateur d'horloge.

Dans le mode préféré de réalisation décrit ici, ce facteur multiplicateur d'horloge est égal respectivement à 1, 2 et 3 pour les valeurs des couplets (bit3, bit4) respectivement égales à (0,1), (1,0), (1,1).

Dans le mode de réalisation particulier décrit ici, ce facteur multiplicateur est mémorisé dans le registre mult_horl de la zone utilisable 110 de la mémoire EEPROM, ce registre étant lu par le processeur CPU à la mise sous tension pour paramétrer le composant PLL.

Dans le mode de réalisation décrit ici, la carte à microcircuit comporte des moyens de modification adaptés à permettre ou à empêcher l'utilisation d'une fonction logicielle f de la carte.

En pratique, la mémoire morte ROM comporte un programme informatique pouvant invoquer cette fonction logicielle f lorsqu'un registre soft de la zone utilisable 110 de la mémoire non volatile EEPROM contient la valeur 1.

Sur réception de la commande 200, le processeur CPU lit, écrit dans le registre soft la valeur du cinquième bit bit5 de l'ordre prédéterminé reçu dans la commande 200.

Dans l'exemple décrit ici, la fonction logicielle est une fonction cryptographique ou une fonction de contrôle d'une signature de données numériques reçues par les moyens de réception RX.

La carte à microcircuit 100 comporte aussi des moyens de modification adaptés à permettre ou empêcher l'utilisation de tout ou partie d'un circuit électronique 120 de la carte.

Dans le mode de réalisation décrit ici, ce circuit électronique 120 comporte une unité cryptographique.

En pratique, l'utilisation de ce circuit électronique 120 est possible après écriture de la valeur 1 dans un registre hard de ce composant, la valeur de ce registre étant modifiée par le processeur CPU avec le contenu du sixième bit bit6 de l'ordre prédéterminé.

Dans l'exemple décrit ici, la modification de la fréquence d'horloge, l'autorisation ou l'empêchement d'utiliser la fonction logicielle ou le composant électronique sont des opérations réversibles. Dans un autre mode de réalisation, l'une au moins de ces opérations pourrait ne pas être réversible.

Nous allons maintenant décrire en référence à la **figure 3**, les principales étapes d'un procédé de configuration conforme à l'invention dans un mode préféré de réalisation.

Le procédé de configuration comporte une première étape E10 de personnalisation. Cette étape est connue de l'homme du métier, et ne sera décrite en détail ici.

Quoi qu'il en soit, cette étape de personnalisation consiste à écrire dans une mémoire de la carte, par exemple dans l'EEPROM des données spécifiques à cette carte ou à un utilisateur de cette carte.

Dans l'exemple décrit ici, cette étape de personnalisation comprend en particulier l'écriture dans une mémoire EEPROM de la carte à microcircuit 100 la valeur de la clef d'authentification AUTH.

Cette étape de personnalisation comprend aussi la création du fichier FICHIER_VOID et de sa clé 220 dans la mémoire EEPROM.

L'étape E10 est suivie par une étape E20 de réception de la commande 200 décrite précédemment en référence à la figure 2.

L'étape E20 est suivie par une étape de vérification E30 au cours de laquelle le processeur CPU authentifie un émetteur de la commande 200. Cette étape d'authentification s'effectue, dans le mode de réalisation décrit ici, en vérifiant si la commande 200 a été cryptée avec une clef d'authentification AUTH prédéterminée, la clef d'authentification AUTH étant mémorisée dans un registre de la mémoire EEPROM au moment de la personnalisation de la carte.

Si tel n'est pas le cas, le résultat du test E30 est négatif. Ce test est alors suivi par l'étape E20 de réception d'une commande déjà décrite.

En revanche, si l'émetteur de la commande 200 est authentifié comme autorisé à émettre la commande 200, le résultat du test E30 est positif.

Ce test est alors suivi par un test E35 au cours duquel on vérifie l'unicité de la commande 200. Ce test E35 de vérification permet d'éviter qu'une commande 200 déjà reçue et copiée frauduleusement ne soit prise en compte une deuxième fois de façon non autorisée.

De façon connue, ce test E35 de vérification peut être mis en œuvre en incorporant un numéro de message dans chaque commande 200, ce

numéro étant incrémenté pour chaque commande, et en comparant ce numéro reçu dans une commande 200 particulière, avec la valeur du numéro reçu dans la commande 200 précédente.

Si la commande 200 a déjà été reçue, le résultat du test de vérification E35 est négatif. Ce test est alors suivi par l'étape E20 de réception d'une commande 200 déjà décrite.

En revanche, si la commande 200 est reçue pour la première fois, le résultat du test de vérification E35 est positif.

Ce test est alors suivi par une étape E40 au cours de laquelle on modifie, la taille de la zone utilisable 110 de la mémoire physique EEPROM en fonction des valeurs des premier et deuxième bits (bit1, bit2) de l'ordre prédéterminé 210 reçu dans la commande 200.

Selon les différentes variantes de réalisations décrites précédemment en référence à la figure 1, cette étape E40 est réalisée, en créant, en détruisant le fichier FICHIER_VOID contenu dans la mémoire physique EEPROM, ou en modifiant la taille de ce fichier FICHIER_VOID.

L'étape E40 de modification de la taille de la zone utilisable 110 de la mémoire physique EEPROM est suivie par une étape E60 au cours de laquelle on mémorise le facteur multiplicateur de la fréquence de l'horloge externe CLOCK dans le registre mult_horl de la zone utilisable 110 de la mémoire EEPROM, ce registre étant lu par le processeur CPU à la mise sous tension pour paramétrer le composant PLL, ce qui a pour effet de modifier, de façon réversible la fréquence d'horloge de la carte.

Comme décrit précédemment, le facteur de multiplicateur de cette fréquence d'horloge est déterminé par la valeur du troisième bit bit3 et du quatrième bit bit4 de l'ordre 210 prédéterminé.

L'étape E60 de modification de la fréquence d'horloge est suivie par une étape E70 au cours de laquelle le processeur CPU écrit dans le registre soft de la mémoire non volatile EEPROM la valeur du cinquième bit bit5 de l'ordre 210.

Comme décrit précédemment, lorsque ce registre soft mémorise la valeur 1, une fonction logicielle f par exemple une fonction cryptographique

telle qu'une fonction de contrôle d'une signature de données numériques est rendue accessible en ce qu'elle peut être invoquée par un programme informatique mémorisé dans la mémoire ROM ou la mémoire EEPROM.

L'étape E70 est suivie par une étape E80 au cours de laquelle le processeur CPU mémorise dans le registre hard du circuit électronique 120 la valeur du sixième bit bit6 de l'ordre prédéterminé.

Lorsque ce registre hard mémorise la valeur 1, l'utilisation de ce circuit électronique 120 est autorisé. Dans le mode de réalisation préféré décrit ici, ce circuit électronique 120 est une unité cryptographique.

L'étape E80 est suivie par l'étape E20 de réception d'une commande déjà décrite.

REVENDICATIONS

1. Carte à microcircuit (100) comportant des moyens (RX) de réception d'une commande (200) et des moyens de modification d'au moins une performance de ladite carte sur réception de ladite commande, les moyens de modification étant caractérisés en ce qu'ils peuvent être mis en œuvre après une étape (E10) de personnalisation de ladite carte.

2. Carte à microcircuit selon la revendication 1, caractérisée en ce qu'elle comporte en outre des moyens d'authentification d'un émetteur de ladite commande (200).

3. Carte à microcircuit selon la revendication 1 ou 2, caractérisée en ce que les moyens de modification sont adaptés à déterminer ladite au moins une performance en fonction d'un ordre prédéterminé (210) reçu dans ladite commande (200).

4. Carte à microcircuit selon l'une quelconque des revendications 1 à 3, caractérisée en ce que lesdits moyens de réception (RX) sont adaptés à recevoir ladite commande (200) selon un protocole de type SMS.

5. Carte à microcircuit selon l'une quelconque des revendications 1 à 4, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à modifier la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) de ladite carte.

6. Carte à microcircuit selon la revendication 5, caractérisée en ce que ladite modification de la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) est effectuée en créant ou en détruisant au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique, ou

en modifiant la taille d'au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique.

7. Carte à microcircuit selon l'une quelconque des revendications 1 à 6, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à modifier, de façon réversible ou non, une fréquence d'horloge de ladite carte.

8. Carte à microcircuit selon l'une quelconque des revendications 1 à 7, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à permettre ou empêcher, de façon réversible ou non, l'utilisation d'au moins une fonction logicielle (f) de ladite carte.

9. Carte à microcircuit selon l'une quelconque des revendications 1 à 8, caractérisée en ce que lesdits moyens de modification d'au moins une performance sont adaptés à permettre ou empêcher, de façon réversible ou non, l'utilisation de tout ou partie d'un circuit électronique (120) de ladite carte.

10. Carte à microcircuit selon la revendication 9, caractérisée en ce que ledit circuit électronique (120) est une unité cryptographique.

11. Carte à microcircuit selon l'une quelconque des revendications 1 à 10, caractérisée en ce qu'elle comporte en outre des moyens de synchronisation (130) adaptés à vérifier l'unicité de ladite commande (200).

12. Procédé de configuration d'une carte à microcircuit (100) caractérisé en ce qu'il comporte les étapes successives suivantes :

- personnalisation (E10) de ladite carte ;
- réception (E20) d'une commande (200) ; et
- modification (E40, E60, E70, E80) d'au moins une performance de la carte sur réception de ladite commande (200).

13. Procédé de configuration selon la revendication 12, caractérisé en ce que ladite étape de réception (E20) est suivie par une étape (E30) d'authentification d'un émetteur de ladite commande (200).

14. Procédé de configuration selon la revendication 12 ou 13, caractérisé en ce que, au cours de ladite étape de modification (E40, E60, E70, E80), on détermine ladite au moins une performance en fonction d'un ordre prédéterminé (210) reçu dans ladite commande (200).

15. Procédé de configuration selon l'une quelconque des revendications 12 à 14, caractérisé en ce que ladite étape (E20) de réception d'une commande (200) est conforme à un protocole de type SMS.

16. Procédé de configuration selon l'une quelconque des revendications 12 à 15, caractérisé en ce que, au cours de ladite étape (E40) de modification d'au moins une performance, on modifie la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) de ladite carte.

17. Procédé de configuration selon la revendication 16, caractérisé en ce que au cours de ladite modification de la taille d'une zone utilisable (110) d'une mémoire physique (EEPROM) , on crée ou on détruit au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique ou on modifie la taille d'au moins un fichier spécifique (FICHIER_VOID) compris dans ladite mémoire physique.

18. Procédé de configuration selon l'une quelconque des revendications 12 à 17, caractérisé en ce que, au cours de ladite étape (E60) de modification d'au moins une performance, on modifie, de façon réversible ou non, une fréquence d'horloge de ladite carte.

19. Procédé de configuration selon l'une quelconque des revendications 12 à 18, caractérisé en ce que, au cours de ladite étape (E70) de modification d'au moins une performance, on permet ou en empêche, de façon réversible ou non, l'utilisation d'au moins une fonction logicielle (f) de ladite carte.

20. Procédé de configuration selon l'une quelconque des revendications 12 à 19, caractérisé en ce que, au cours de ladite étape (E80) de modification d'au moins une performance, on permet ou en empêche, de façon réversible ou non, l'utilisation de tout ou partie d'un circuit électronique (120) de ladite carte.

21. Procédé de configuration selon la revendication 20, caractérisé en ce que ledit composant électronique (120) est une unité cryptographique.

22. Procédé de configuration selon l'une quelconque des revendications 12 à 21, caractérisé en ce qu'il comporte , préalablement à ladite étape (E40) de modification d'au moins une performance, une étape (E35) de vérification de l'unicité de ladite commande (200).

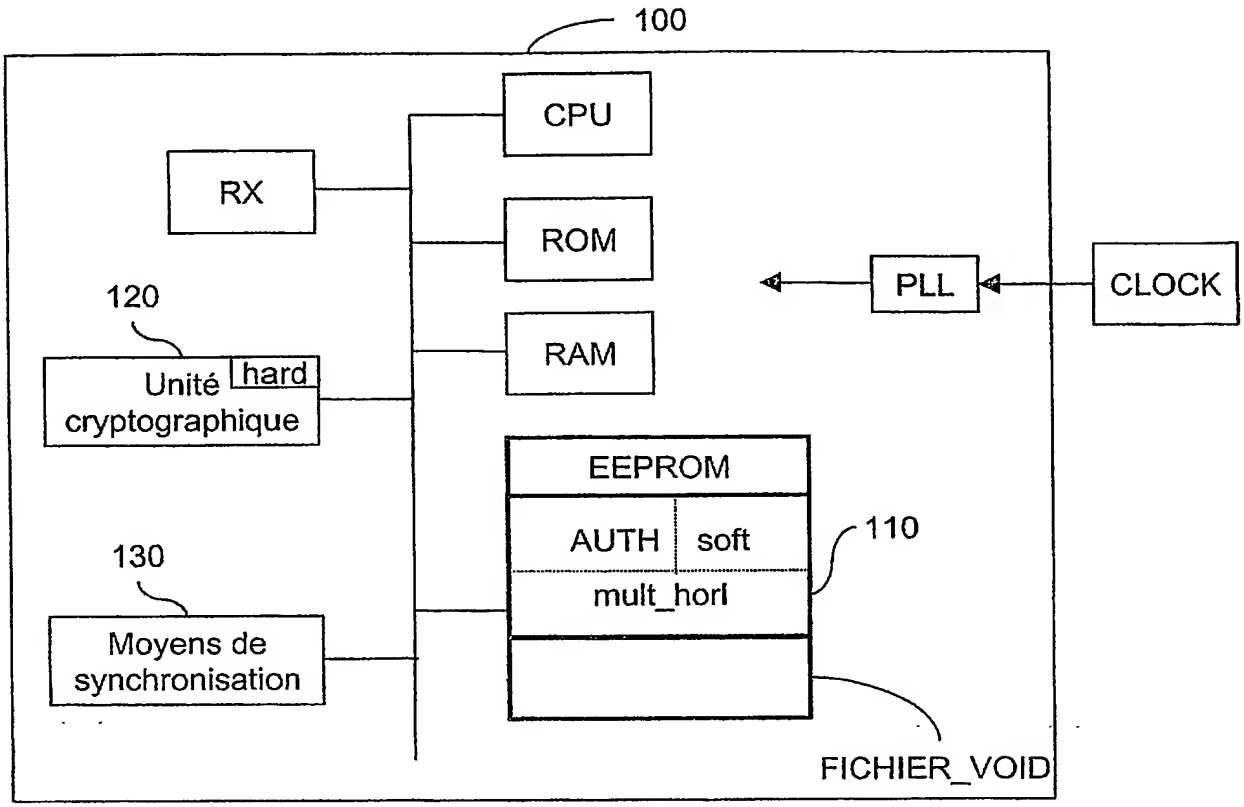


FIGURE 1

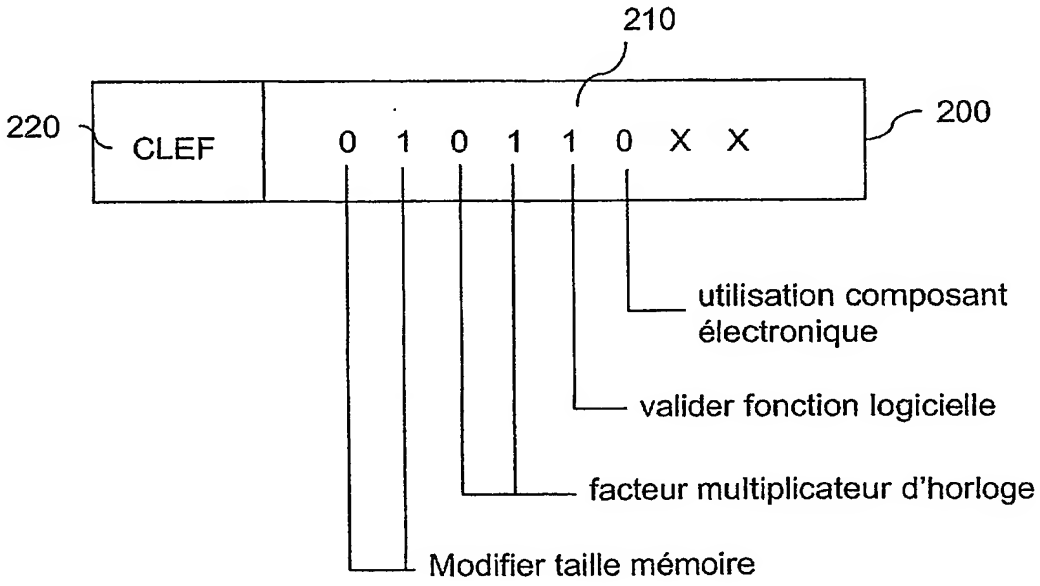


FIGURE 2

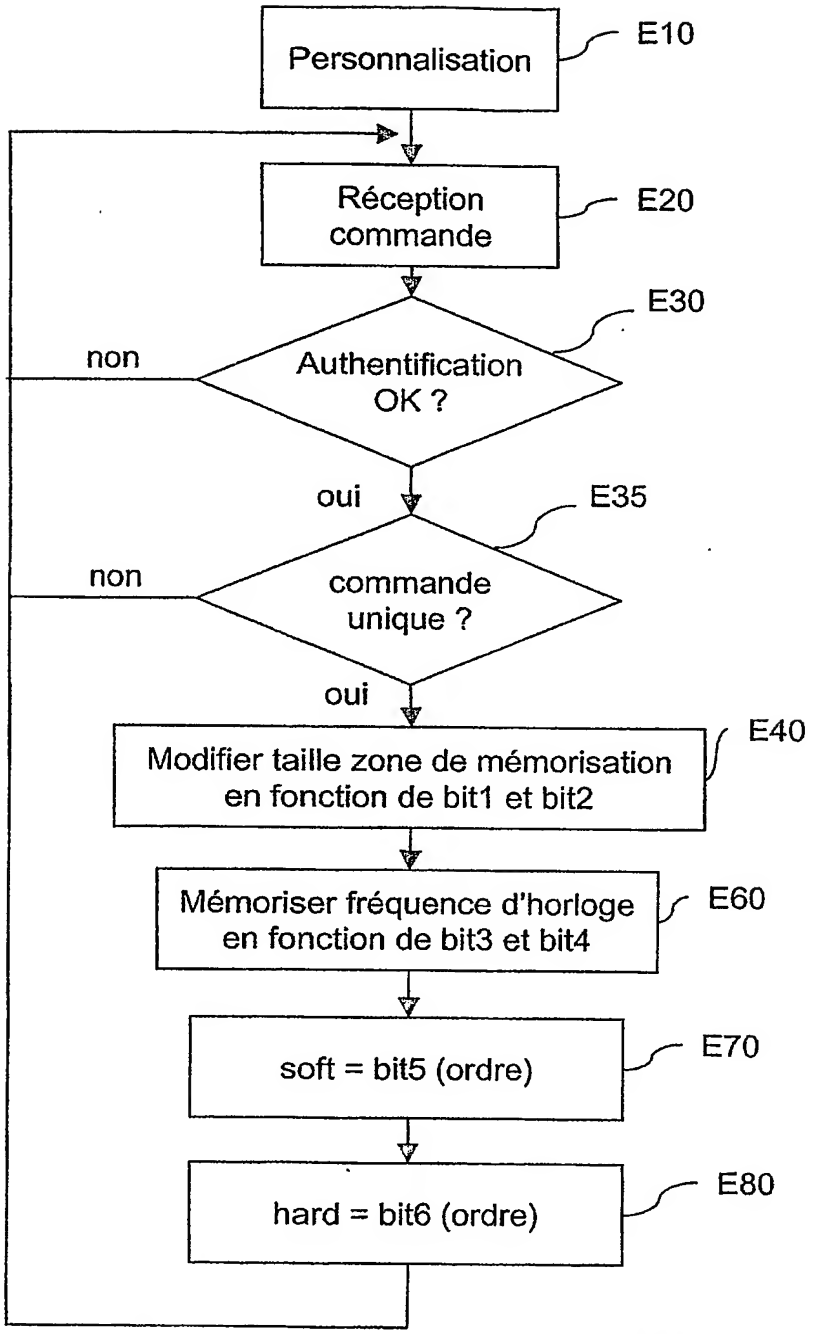

Personnalisation
E10
Réception commande
E20
Authentification OK ?
E30
non
oui
commande unique ?
E35
non
oui
Modifier taille zone de mémorisation en fonction de bit1 et bit2
E40
Mémoriser fréquence d'horloge en fonction de bit3 et bit4
E60
soft = bit5 (ordre)
E70
hard = bit6 (ordre)
E80

FIGURE 3

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTI[illegible]

Code de la propriété intellectuelle - Livre VI

N° 11235*03

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

CB 113 W / 270600

Vos références pour ce dossier *(facultatif)*	BIF114642/FR
N° D'ENREGISTREMENT NATIONAL	02.12.340

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Carte à microcircuit dont les performances peuvent être modifiées après personnalisation.

LE(S) DEMANDEUR(S) :

OBERTHUR CARD SYSTEMS SA

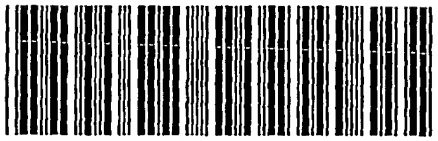
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		JAYET
Prénoms		Stéphane
Adresse	Rue	25, allée des Noisetiers,
	Code postal et ville	95250 BEAUCHAMP, France.
Société d'appartenance *(facultatif)*		
2 Nom		HUOT
Prénoms		Jean-Claude
Adresse	Rue	14, rue Hoche,
	Code postal et ville	78350 JOUY-EN-JOSAS, France.
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

Le 4 Octobre 2002
Bruno QUANTIN N°92.1206
CABINET BONNET-THIRION



BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [x] IMAGE CUT OFF AT TOP; BOTTOM OR SIDES
- [x] FADED TEXT OR DRAWING
- [ ] BLURED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [x] COLORED OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [ ] LINES OR MARKS ON ORIGINAL DOCUMENT
- [ ] REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox